a step of erasing both the internal encryption key stored in the image input apparatus and the external encryption key stored in said plurality of storage means coincident with completion of the step of encrypting the internal encryption key.

REMARKS

This application has been carefully reviewed in light of the Office Action dated June 20, 2002. Claims 1 to 14, 18 to 20 and 22 remain in the application, of which Claims 1, 4, 8 to 10, 12, 14, 18, 20 and 22 have been amended. Claims 1, 10, 14, 18, 20 and 22 are the independent claims herein. Reconsideration and further examination are respectfully requested.

Claims 18 and 19 were rejected under 35 U.S.C. § 112, second paragraph for a typographical error that has been attended to by amendment. Withdrawal of the rejection is respectfully requested.

Claims 1 to 3, 5, 6, 8, 10 to 14, 18, 20 and 22 were rejected under 35 U.S.C. § 103(a) over U.S. Patent No. 5,535,277 (Shibata) in view of U.S. Patent No. 5,870,468 (Harrison), Claim 4 was rejected over Shibata in view of Harrison and further in view of Official Notice taken by the Examiner, and Claims 7, 9 and 19 were rejected over Shibata in view of Harrison and further in view of an article to Schneier. Each of the independent claims have been amended merely to more clearly recite subject matter which is already implicitly, if not explicitly, recited in the claims. As such, the rejections are traversed, and the Examiner is respectfully requested to reconsideration and withdrawal the rejections after considering the following.

The present invention concerns encryption of digital information. According to one aspect of the invention, an external encryption key used to encrypt the digital information is erased from each of two different storage means (such as a control program memory and a working memory; see page 21, lines 10 to 18) in which the key is stored. In another aspect, an external key is used to encrypt an internal key, with both keys being erased. In both aspects, the key(s) is/are erased coincident with completion of the encryption process. As a result, a time lag between the encryption process and erasing of the encryption key(s) is significantly reduced and the likelihood of a hacker being able to obtain the encryption key(s) is reduced.

With specific reference to the claims, amended independent Claim 1 is an image input apparatus comprising conversion means for converting an image signal into digital information, reading means for reading an encryption key from an external source, first storage means for storing the encryption key read by the reading means, second storage means for storing the encryption key to execute an encryption process, encryption means for encrypting the digital information by using the encryption key stored in the second storage means, and erasing means for erasing the encryption key from the first and second storage means coincident with completion of the digital information being encrypted by the encryption means.

Amended independent Claims 10 and 14 are method and computer program claims, respectively, that substantially correspond to Claim 1.

Amended independent Claim 18 is an image input apparatus comprising conversion means for converting an image signal into digital information, information

encryption means for encrypting the digital information by using an internal encryption key stored within the image input apparatus, means for inputting from an external source an external encryption key for encrypting the internal encryption key, key encryption means for encrypting the internal encryption key by using the external encryption key and storing the external encryption key in a plurality of storage means, and erasing means for erasing both the internal encryption key stored in the image input apparatus and the external encryption key stored in the plurality of storage means coincident with completion of encrypting the internal encryption key by the key encryption means.

Amended independent Claims 20 and 22 are method and computer program claims, respectively, that substantially correspond to Claim 18.

The applied art, alone or in combination, is not seen to disclose or to suggest the features of independent Claims 1, 10, 14, 18, 20 and 22. More particularly, the applied art is not seen to disclose or to suggest at least the feature of erasing an external encryption key, which is read from an external source, from both a first and a second storage means in which the key is stored coincident with completion of digital information being encrypted (Claims 1, 10 and 14), or erasing both an internal encryption key stored in an image input apparatus and an external encryption key stored in a plurality of storage means coincident with completion of encrypting the internal encryption key with the external encryption key (Claims 18, 20 and 22).

Shibata is seen to disclose that an encryption/decryption circuit 403 encrypts data using an encryption key maintained by the circuit. After encryption is completed, the encrypted data is transmitted over a phone line. In Shibata, a user can register (i.e., create),

change and delete an encryption key by assigning a ten-digit number. The user performs these processes via an operation section 7. (See column 4, lines 48 to 51 and column 7, lines 39 to 45.) However, the encryption key used to encrypt the data in Shibata is maintained in the device (i.e., it is an internal key) and is not a key from an external source. Therefore, Shibata is not seen to disclose or to suggest at least the feature of erasing an external encryption key, which is read from an external source, from both a first and a second storage means in which the key is stored coincident with completion of digital information being encrypted (Claims 1, 10 and 14), or erasing both an internal encryption key stored in an image input apparatus and an external encryption key stored in a plurality of storage means coincident with completion of encrypting the internal encryption key with the external encryption key (Claims 18, 20 and 22).

Harrison is merely seen to disclose that files are encrypted with an encryption key and two scrambled versions of the encryption key are stored in the computer, one scrambled with a secret key and the other scrambled with a transform of the secret key. The unscrambled version of the encryption key is then erased from the computer's memory, but the scrambled versions of the encryption key remain in the computer. When a user enters the proper secret key, the scrambled versions are unscrambled and the encryption key is restored in the computer and used to decrypt any encrypted files. Thus, Harrison makes multiple versions (copies) of the encryption key and only erases one of those versions, with the other versions of the encryption key remaining in the computer, albeit in a scrambled format, which are later used to restore the encryption key. (See column 4, lines 30 to 47, and column 6, lines 43 to 52.) As such, Harrison

cannot reasonably be seen to correspond to the present invention and therefore is not seen to disclose or to suggest at least the feature of erasing an external encryption key, which is read from an external source, from both a first and a second storage means in which the key is stored coincident with completion of digital information being encrypted (Claims 1, 10 and 14), or erasing both an internal encryption key stored in an image input apparatus and an external encryption key stored in a plurality of storage means coincident with completion of encrypting the internal encryption key with the external encryption key (Claims 18, 20 and 22).

Moreover, a combination of Shibata and Harrison would change the principal of operation of Harrison and render it useless for its intended purpose, thereby making the proposed combination improper. In this regard, Shibata teaches that a user can delete an encryption key at will, while Harrison teaches that the encryption key remains in the computer at all times in either a scrambled or unscrambled form. The encryption key's presence in Harrison is critical to the ability to encrypt files if the computer becomes idle for a prolonged timeframe. Applying Shibata's teaching of allowing a user to delete an encryption key so that no encryption key is present in the computer would render Harrison useless since no key would be available to encrypt files. Thus, the proposed combination of Shibata and Harrison is mere hindsight reasoning and a prima facie case of obviousness cannot be established from such a combination.

Schneier is not seen to add anything to overcome the deficiencies of Shibata and Harrison and is also not seen to disclose or to suggest at least the feature of erasing an external encryption key, which is read from an external source, from both a first and a

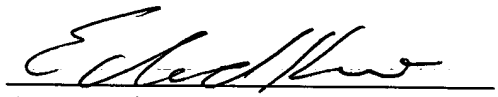
second storage means in which the key is stored coincident with completion of digital information being encrypted (Claims 1, 10 and 14), or erasing both an internal encryption key stored in an image input apparatus and an external encryption key stored in a plurality of storage means coincident with completion of encrypting the internal encryption key with the external encryption key (Claims 18, 20 and 22).

In view of the foregoing amendments and remarks, the entire application is believed to be in condition for allowance and such action is respectfully requested at the Examiner's earliest convenience.

As a formal matter, Applicant notes that the Examiner has not yet returned an initialed copy of the Form PTO-1449 from the April 26, 2000 Information Disclosure Statement. Therefore, Applicant requests that the Examiner return an initialed form with the next communication, and for the Examiner's convenience, a copy of the Form PTO-1449 from the foregoing Information Disclosure Statement is enclosed herewith.

Applicant's undersigned attorney may be reached in our Costa Mesa, California office at (714) 540-8700. All correspondence should continue to be directed to our below-listed address.

Respectfully submitted,



Attorney for Applicant
Registration No. 42,746

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-2200
Facsimile: (212) 218-2200

APPENDIX

VERSION WITH MARKINGS TO SHOW CHANGES MADE TO CLAIMS

1. (Twice Amended) An image input apparatus comprising:

conversion means for converting an image signal into digital information;

reading means for reading an encryption key from an external source;

first storage means for storing said encryption key read by the reading means;

second storage means for storing said encryption key to execute an encryption process;

encryption means for encrypting the digital information by using said [an] encryption key stored in the second storage means; and

erasing means for erasing said encryption key from said first and second storage means coincident with completion of the digital information being encrypted by the encryption means.

4. (Amended) An image input apparatus according to claim 1, further comprising means for inputting said encryption key from [an] the external source.

8. (Amended) An image input apparatus according to claim 1, further comprising means for inputting from [an] the external source another encryption key for encrypting said encryption key.

9. (Amended) An image input apparatus according to claim 8, wherein said encryption key comprises an encryption key based on a common key cryptosystem, and said another encryption key comprises an encryption key based on a public key cryptosystem.

10. (Twice Amended) An image input method comprising the steps of:

converting an image signal into digital information;

reading an encryption key form an external source;

a first storage step of storing said encryption key in a first storage means;

a second storage step of storing said encryption key in a second storage means to execute an encryption process;

encrypting the digital information by using [an] said encryption key stored in said second storage means; and

erasing said encryption key from said first and second storage means coincident with completion of the digital information being encrypted in the encrypting step.

12. (Amended) An image input method according to claim 10, wherein the image signal is generated from an optically picked up image of a subject which is converted into the digital information.

14. (Twice Amended) An encryption processing program stored in a computer-readable medium, comprising:

a step of converting an image signal into digital information;

a step of reading an encryption key from an external source;

a first storage step of storing said encryption key in a first storage means;

a second storage step of storing said encryption key in a second storage means to execute an encryption process;

a step of encrypting the digital information by using [an] said encryption key stored in said second storage means; and

a step of erasing said encryption key from said first and said second storage means coincident with completion of the digital information being encrypted in the encrypting step.

18. (Twice Amended) An image input apparatus comprising:

conversion means for converting an image signal into digital information;

information encryption means for encrypting the digital information by using an internal encryption key [disposed] stored within said image input apparatus;

means for inputting from an external source an external encryption key for encrypting said internal encryption key;

key encryption means for encrypting said internal encryption key by using said external encryption key and storing said external encryption key in a plurality of storage means; and

erasing means for erasing both the internal encryption key stored in the image input apparatus and the external encryption key stored in said plurality of storage means coincident with completion of encrypting the [external] internal encryption key by the key encryption means.

20. (Twice Amended) An image input method for an image input apparatus comprising the steps of:

converting an image signal into digital information;

encrypting the digital information by using an internal encryption key [disposed] stored within said image input apparatus;

obtaining from an external source an external encryption key for encrypting said internal encryption key;

encrypting said internal encryption key by using said external encryption key and storing said external encryption key in a plurality of storage means: and

erasing both the internal encryption key stored in the image input apparatus and the external encryption key stored in said plurality of storage means coincident with

completion of the step of encrypting the internal encryption key using the external encryption key.

22. (Twice Amended) An encryption processing program stored in a computer-readable medium, comprising:

a step of converting an image signal into digital information;

a step of encrypting the digital information by using an internal encryption key [disposed] stored within an image input apparatus;

a step of obtaining from an external source an external encryption key for encrypting said internal encryption key;

a step of encrypting said internal encryption key by using said external encryption key and storing said external encryption key in a plurality of storage means; and

a step of erasing both the internal encryption key stored in the image input apparatus and the external encryption key stored in said plurality of storage means coincident with completion of the step of encrypting the internal encryption key.

FORM PTO 1449 (*modified*)

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE

LIST OF REFERENCES CITED BY APPLICANT(S)
(Use several sheets if necessary)

ATTY DOCKET NO. **35.G2331**	APPLICATION NO. **09/222,846**
APPLICANT **KAZUOMI OISHI**	
FILING DATE **December 30, 1998**	GROUP **3642**

U.S. PATENT DOCUMENTS

*EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE

FOREIGN PATENT DOCUMENTS

		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION YES/NO/ OR ABSTRACT

OTHER DOCUMENT(S) (Including Author, Title, Date, Pertinent Pages, Etc.)

		R.L. Rivest, A. Schami and L. Adleman, "A Method Of Obtaining Digital Signatures And Public Key Cryptosystems", Communications of the ACM, February 1978, Vol. 21, No. 2, pages 120-126.

EXAMINER	DATE CONSIDERED

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.